PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-021302
(43)Date of publication of application : 23.01.1998

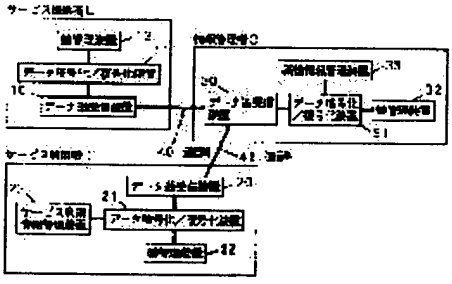
(51)Int.Cl. G06F 17/60
G06F 1/00
G06F 15/00
G06F 17/00
G09C 1/00
G09C 1/00
H04L 9/32

(21)Application number : 08-174709
(22)Date of filing : 04.07.1996

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : OKUMURA YASUO
MIYAJI MITSUKO

(54) USER'S INFORMATION COLLECTING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To enable a service provider to safely acquire service utilizing information used by a service utilizing and attribute information (age, an annual income, a carrier, etc.), stored in a third person by cipher communication while guaranteeing the anonymity of the user.
SOLUTION: The system is composed of a service provider L, a service utilizer I and an information manager C for storing the attribute information bi of the user I. The manager C ciphers service utilizing information ai to the provider L and management information di is connected to the ciphered information ai to cipher the connected information of the provider L. The provider L decodes data, extracts an identification number di, connects corresponding attribute information bi to the ciphered service utilizing information ai to cipher information to the provider L. The provider L decodes the received data twice and acquires the service utilizing information ai and the attribute information bi while guaranteeing the anonymity of the user I.



LEGAL STATUS

[Date of request for examination] 03.03.2003

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－21302

(43)公開日　平成10年(1998)１月23日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	17/60			Ｇ０６Ｆ	15/21	Ｚ
	1/00	３７０			1/00	３７０Ｅ
	15/00	３３０			15/00	３３０Ａ
	17/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｚ
Ｇ０９Ｃ	1/00	６４０	7259－5Ｊ			６６０Ｅ

審査請求　未請求　請求項の数10　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願平8－174709

(22)出願日　平成８年(1996)７月４日

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　奥村　康男
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　宮地　充子
大阪府門真市大字門真1006番地　松下電器産業株式会社内

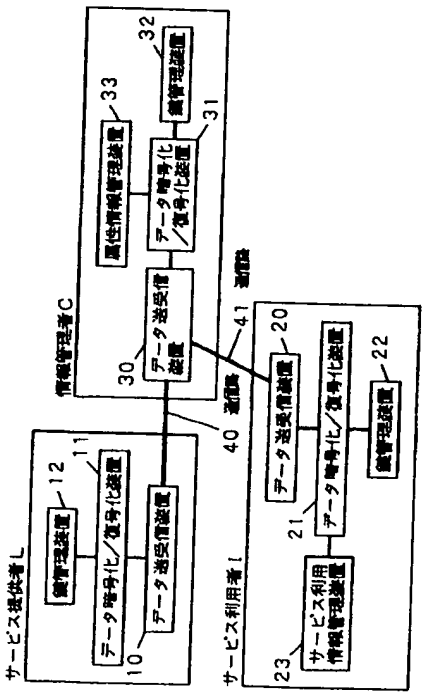
(74)代理人　弁理士　滝本　智之　(外１名)

(54)【発明の名称】　利用者情報収集システム

(57)【要約】

【課題】　サービス提供者が、サービス利用者が利用したサービス利用情報と第三者の保持する利用者の属性情報(年齢、年収、学歴等)を利用者の匿名性を保証した上で暗号通信により安全に入手する。

【解決手段】　サービス提供者L、サービス利用者I、サービス利用者Iの属性情報biを保持する情報管理者Cで構成する。情報管理者Cはサービス利用情報aiをサービス提供者Lに向けて暗号化し、暗号化したサービス利用情報aiに管理情報diを連結し、情報管理者Cに向けて暗号化する。情報管理者Cはデータを復号して識別番号diを取り出し、対応する属性情報biと暗号化サービス利用情報aiを連結させサービス提供者Lに向けて暗号化する。サービス提供者Lは受信したデータを二度復号し、サービス利用情報aiと属性情報biをサービス利用者Iの匿名性を保証した上で入手する。



1

【特許請求の範囲】

【請求項１】サービス提供者Lと、前記サービス提供者Lの提供するサービスを利用するサービス利用者Iと、前記サービス利用者Iに関する属性情報biを管理する情報管理者Cからなり、データを送受信する通信路と、電子的なデータを暗号化および復号化できるデータ暗号化／復号化装置を用い、前記サービス提供者Lが、前記サービス利用者Iを特定することなく、前記サービス提供者Lの提供するサービス利用情報aiと、そのサービスを利用したサービス利用者の利用者属性情報biとを入手できることを特徴とする利用者情報収集システム。

【請求項２】前記情報管理者Cは、サービス利用者の識別番号diとこれに対応する前記属性情報biを管理する属性情報管理装置を備え、前記サービス利用者Iは、サービス利用者の識別番号diとこれに対応する前記サービス利用情報aiを管理するサービス利用情報管理装置を備え、前記サービス利用者Iは、第1のデータ暗号化装置において、前記サービス利用情報管理装置において管理されている前記サービス利用情報aiを、第1の鍵管理装置において管理されている前記サービス提供者L向けの暗号鍵PILで暗号化して暗号化サービス利用情報E(ai, PIL)を作成し、前記暗号化サービス利用情報E(ai, PIL)と前記識別番号diとを連結したデータE(ai, PIL)||diを、前記第1のデータ暗号化装置において、第1の鍵管理装置において管理されている前記情報管理者C向けの暗号鍵PICで暗号化し、暗号化データE(E(ai, PIL)||di, PIC)を、第1のデータ送受信装置より前記情報管理者Cに向けて送信し、前記情報管理者Cは、前記サービス利用者Iから送信された前記暗号化データE(E(ai,PIL)||di, PIC)を第2のデータ送受信装置において受信し、前記暗号化データE(E(ai, PIL)||di, PIC)を第2のデータ復号化装置において、第2の鍵管理装置において管理されている前記サービス利用者Iからの通信用の前記情報管理者Cの復号鍵SCIで復号化し、前記暗号化サービス利用情報E(ai, PIL)と前記識別番号diを取り出し、前記属性情報管理装置において、前記識別番号diに対応する属性情報biを読み出し、前記暗号化サービス利用情報E(ai, PIL)と前記属性情報biとを連結したデータE(ai, PIL)||biを作成し、第2のデータ暗号化装置において、前記データE(ai, PIL)||biを、前記第2の鍵管理装置において管理されている前記サービス提供者L向けの暗号鍵PCLで暗号化して暗号化データE(E(ai, PIL)||bi, PCL)を作成し、これを、前記第2のデータ送受信装置より前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(E(ai, PIL)||bi, PCL)を第3のデータ送受信装置において受信し、これを、第3のデータ復号装置において、第3の鍵管理装置において管理されている前記情報管理者Cからの通信用のサービス提供者Lの復号鍵SLCで復号し、前記暗号化サービス利用情報E(ai, PIL)と前記属性情報biを取り出し、前記

2

暗号化サービス利用情報E(ai, PIL)を、前記第3のデータ復号装置において、前記第3の鍵管理装置おいて管理されている前記サービス利用者Iからの通信用のサービス提供者Lの復号鍵SLIで復号し、サービス利用情報aiを取り出し、前記サービス利用情報aiとそれに対応するサービス利用者Iの属性情報biを、サービス利用者Iを特定することなく得ることを可能にすることを特徴とする請求項１記載の利用者情報収集システム。

【請求項３】前記情報管理者Cは、前記サービス利用者Iの識別番号diとこれに対応する前記属性情報biを管理する属性情報管理装置を備え、前記サービス提供者Lは、前記サービス利用者Iの識別番号diとこれに対して提供したサービス利用情報aiを管理するサービス利用情報管理装置を備え、前記サービス提供者Lは、あるサービス利用情報aiに関連する任意のn人(n ≧ 2)のサービス利用者I1,...,Inに対する識別番号d1,...,dnを連結したデータd1||…||dnを、第3のデータ暗号化装置において、第3の鍵管理装置において管理されている前記情報提供者C向けの暗号鍵KCによって暗号化して、暗号化データE(d1||…||dn, KC)を作成し、これを前記情報管理者Cに送信し、前記情報管理者Cは、前記サービス提供者Lから送信された前記暗号化データE(d1||…||dn,KC)を受信し、これを第2のデータ復号装置おいて、第2の鍵管理装置において管理されている前記サービス提供者Lからの通信用の情報管理者Cの復号鍵DCで復号し、d1||…||dnを取り出し、その内容である、前記識別番号(d1,....dn)のそれぞれに対応する属性情報(b1,....,bn)を、前記属性情報管理装置において読み出し、不規則な順序に並び変えて結合しb1'||…||bn'を作成し、第2のデータ暗号化装置において、第2の鍵管理装置において管理されている前記サービス提供者L向けの暗号鍵KLによって暗号化して、暗号化データE(b1'||…||bn', KL)を作成し、これを前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(b1'||…||bn', KL)を受信し、これを第3のデータ復号装置において、第3の鍵管理装置において管理されている前記情報管理者Cからの通信用の前記サービス提供者Lの復号鍵DLで復号化し、不規則に並び換えられた形態で、前記識別番号d1,....dnのサービス利用者I1,...Inに対する属性情報b1',....bn'を取り出し、これによりサービス利用情報aiとこれに対応するサービス利用者Iの属性情報biを、サービス利用者Iを特定することなく得ることを特徴とする請求項１記載の利用者情報収集システム。

【請求項４】前記サービス提供者Lと前記サービス利用者Iとの間で鍵KLIを共有し、前記サービス利用者Iと前記情報管理者Cとの間で鍵KICを共有し、前記情報管理者Cと前記サービス提供者Lとの間で鍵KCLを共有し、前記サービス利用者Iは、前記サービス利用情報aiを前記共有鍵KLIで暗号化したデータE(ai, KLI)と前記識別番号d

3

iの連結を前記共有鍵KICで暗号化したデータE(E(ai, KLI)||di, KIC)を前記情報管理者Cに送信し、前記情報管理者Cは、前記サービス利用者Iから送信された暗号化データE(E(ai, KLI)||di, KIC)を前記共有鍵KICで復号し、暗号化データE(ai, KLI)と前記識別番号diを得て、前記識別番号diに対応する前記属性情報biを前記属性管理装置から読み出し、前記属性情報biと暗号化データE(ai, KLI)の連結E(ai, KLI)||biを、前記共有鍵KCLで暗号化し、暗号化データE(E(ai, KLI)||bi, KCL)を前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された暗号化データE(E(ai, KLI)||bi,KCL)を前記共有鍵KCLで復号し、E(ai, KLI)とbiを得た後、前記共有鍵KLIでaiを復号することにより、前記サービス利用情報aiとそれに対応するサービス利用者Iの属性情報biを、前記サービス利用情報aiと属性情報biからは、どのサービス利用者Iに関する情報であるかを特定できない状態で得ることを可能とすることを特徴とする請求項２記載の利用者情報収集システム。

【請求項５】前記サービス提供者L、前記サービス利用者I、前記情報管理者Cは、それぞれ公開鍵PLと秘密鍵SL、PIとSI、PCとSCを保持し、前記サービス利用者Iは、前記サービス利用情報aiを、前記サービス提供者Lの公開鍵PLで暗号化したサービス利用情報E(ai, PL)を作成し、前記暗号化サービス利用情報E(ai, PL)と前記識別番号diとを連結したデータE(ai, PL)||diを、前記情報管理者Cの公開鍵PCで暗号化し、暗号化データE(E(ai, PL)||di, PC)を、前記第１のデータ送受信装置より前記情報管理者Cに向けて送信し、前記情報管理者Cは、前記サービス利用者Iから送信された前記暗号化データE(E(ai, PL)||di, PC)を前記情報管理者Cの秘密鍵SCで復号化し、前記暗号化サービス利用情報E(ai, PL)と前記識別番号diを取り出し、前記属性情報管理装置において、前記識別番号diに対応する前記属性情報biを読み出し、前記暗号化サービス利用情報E(ai, PL)と前記属性情報biとを連結したデータE(ai, PL)||biを、前記サービス提供者Lの公開鍵PLで暗号化したデータE(E(ai, PL)||bi, PL)を作成し、前記暗号化データE(E(ai, PL)||bi), PL)を、前記第2のデータ送受信装置より前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Iから送信された前記暗号化データE(E(ai, PL)||bi, PL)を、前記サービス提供者Lの秘密鍵SLで復号化し、前記暗号化サービス利用情報E(ai, PL)と前記属性情報biを取り出し、前記暗号化サービス利用情報E(ai, PL)を、前記秘密鍵SLで復号化し、サービス利用情報aiを取り出すことにより、前記サービス利用情報aiとそれに対応するサービス利用者Iの属性情報biを、前記サービス利用情報aiと属性情報biからは、どのサービス利用者Iに関する情報であるかを特定できない状態で得ることを可能にすることを特徴とする請求項２記載の利用者情報収集システム。

4

【請求項６】前記サービス提供者L及び前記情報管理者Cは、共有鍵Kを保持し、前記サービス提供者Lは、あるサービス利用情報aiに関連する任意のn人(n ≧2)のサービス利用者I1,...,Inに対する識別番号d1,...,dnを連結したデータd1||…||dnを前記共有鍵Kで暗号化したデータE(d1||…||dn, K)を前記情報管理者Cに送信し、前記情報管理者Cは、前記サービス提供者Lから送信された前記暗号化データE(d1||…||dn,K)を前記共有鍵Kで復号化し、前記識別番号(d1,...,dn)のそれぞれに対応する属性情報(b1,...,bn)を、前記属性情報管理装置において読み出し、不規則な順序に並び変えた後に結合してb1'||…||bn'を作成し、前記共有鍵Kで暗号化したデータE(b1'||…||bn', K)を前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(b1'||…||bn', K)を共有鍵Kで復号化し、不規則に並び換えられた形態で、前記識別番号d1,...,dnのサービス利用者I1,...,Inに対する属性情報b1',...,bn'を、利用者Iを特定できない状態で得ることを特徴とする請求項３記載の利用者情報収集システム。

【請求項７】前記サービス提供者L、前記情報管理者Cは、それぞれ公開鍵PLと秘密鍵SL、PCとSCを管理し、前記サービス提供者Lは、あるサービス利用情報aiに関連する任意のn人(n ≧ 2)のサービス利用者I1,...,Inに対する識別番号d1,...,dnを連結したデータd1||…||dnを前記情報管理者Cの公開鍵PCで暗号化したデータE(d1||…||dn, PC)を前記情報管理者Cに送信し、前記情報管理者Cは、前記サービス提供者Lから送信された前記暗号化データE(d1||…||dn,PC)を秘密鍵SCで復号化し、前記識別番号(d1,...,dn)のそれぞれに対応する属性情報(b1,...,bn)を、前記属性情報管理装置から読み出し、不規則な順序に並び変えた後に結合してb1'||…||bn'を作成し、前記サービス提供者Lの公開鍵PLで暗号化したデータE(b1'||…||bn', PL)を前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報提供者Cから送信された前記暗号化データE(b1'||…||bn', PL)を秘密鍵SLで復号化し、不規則に並び換えられた形態で、前記識別番号d1,...dnのサービス利用者I1,...Inに対する属性情報b1',...bn'を、利用者Iを特定できない状態で得ることを特徴とする請求項３記載の利用者情報収集システム。

【請求項８】前記サービス提供者Lと前記サービス利用者Iとの間でサービスとして授受される情報が、電子的なデータであり、前記サービス提供者Lが提供するサービスにはそれぞれサービス番号SIDが割り当てられており、前記サービス提供者Lは、前記サービス番号SIDと提供者署名文SignSIDを連結させたSID||SignSIDをサービス利用情報aiとし、サービス利用情報aiを提供するデータに付加することにより、前記サービス提供者Lが、前記情報管理者Cから送信された前記サービス番号SIDの正当性を確認する手段を付加することを特徴とする請求項

5

２、４、５のいずれか１項に記載の利用者情報収集システム。

【請求項９】前記サービス利用者Iから前記情報管理者Cへ送信するデータは、前記サービス利用者Iが、前記秘密鍵SIで前記暗号化データE(ai, PL)||diに作成した署名S(E(ai, PL)||di, SI)を含み、前記情報管理者Cは、受信データS(E(ai,PL)||di, SI)の正当性を前記サービス利用者Iの公開鍵PIで確認し、前記情報提供者Cから前記サービス提供者Lへ送信するデータには、前記情報提供者Cが、前記秘密鍵SCで前記暗号化データE(ai, PL)||biに作成した署名S(E(ai, PL)||di,SC)を含み、前記サービス提供者Lは、受信データS(E(ai, PL)||di, SC)の正当性をCの公開鍵PCで確認するフェーズを付加することを特徴とする請求項２記載の利用者情報収集システム。

【請求項１０】前記サービス提供者Lから前記情報管理者Cへ送信するデータは、前記サービス利用者Lが、前記秘密鍵SLで前記暗号化データE(d1||…||dn, PC)に作成した署名S(E(d1||…||dn, PC), SL)を含み、前記情報管理者Cは、受信データS(E(d1||…||dn, PC), SL)の正当性を前記サービス提供者Lの公開鍵PLで確認し、前記情報提供者Cから前記サービス提供者Lへ送信するデータには、前記情報提供者Cが、前記秘密鍵SCで前記暗号化データE(b1'||…||bn', PL)に作成した署名S(E(b1'||…||bn', PL), SC)を含み、前記サービス提供者Lは、受信データS(E(b1'||…||bn', PL), SC)の正当性を前記情報管理者Cの公開鍵PCで確認するフェーズを付加することを特徴とする請求項７記載の利用者情報収集システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】サービス提供者が、サービス利用者の匿名性を保証しながら、サービス利用者が利用したサービスに関する情報と、サービス利用者に関する個人的な情報を収集することに関する。

【０００２】

【従来の技術】従来、有料同報通信システム等において、サービス利用したサービスに関する情報（利用時間や取得情報料、取得した情報の内容等）を記録し、サービス利用に対する課金に反映させたり、サービス提供者がサービスの視聴率や取得率を算出する際の基礎データ等に利用していた。

【０００３】

【発明が解決しようとする課題】しかし、サービス提供者が、サービス内容の充実を図ろうとする場合、上記サービス利用情報を収集するのは当然であるが、さらにサービス利用者の属性（年収、職業、出身地、年齢等）に関する情報を収集し、サービスの内容と利用者との相関関係を分析する必要が生じる。このような要求を実現しようとする場合、個人的な情報を収集、管理する際に生じるコストが問題となる。そこで、他の情報管理者が管理する、サービス利用者に関する情報を利用することが考えられるが、この場合、情報管理者が管理する情報が個人的な情報である場合、利用者のプライバシを保護することが課題となる。

6

【０００４】本発明は、サービス提供者が、サービス利用者を特定することなく、サービス利用者のサービス利用情報と、他の情報管理者の管理するサービス利用者の属性情報とを入手することを可能にすることを目的とする。

【０００５】

【課題を解決するための手段】請求項１に係る発明は、サービス提供者Lと、前記サービス提供者Lの提供するサービスを利用するサービス利用者Iと、前記サービス利用者Iに関する属性情報biを管理する情報管理者Cとから構成される利用者情報収集システムである。

【０００６】請求項２および請求項３に係る発明は、請求項１の発明において、情報管理者Cは、サービス利用者の識別番号diとこれに対応する属性情報biを管理する属性情報管理装置を備え、サービス利用者Iは、サービス利用者の識別番号diと利用したサービスに対応するサービス利用情報aiを管理するサービス利用情報管理装置を備え、前記サービス利用者Iは、情報管理者との間でデータの送受信を行なう第１のデータ送受信装置と、電子的なデータからなる鍵を管理する第1の鍵管理装置と、前記鍵を用いて電子的なデータを暗号化する第１のデータ暗号化装置と、前記鍵を用いて暗号化されたデータを復号する第１のデータ復号装置を備え、前記情報管理者Cは、サービス提供者LおよびサービスI利用者Iとの間でデータの送受信を行なう第２のデータ送受信装置と、電子的なデータからなる鍵を管理する第２の鍵管理装置と、前記鍵を用いて電子的なデータを暗号化する第２のデータ暗号化装置と、前記鍵を用いて暗号化されたデータを復号する第２のデータ復号装置を備え、前記サービス提供者Lは、情報管理者Cとの間でデータの送受信を行なう第３のデータ送受信装置と、電子的なデータからなる鍵を管理する第３の鍵管理装置と、前記鍵を用いて電子的なデータを暗号化する第３のデータ暗号化装置と、前記鍵を用いて暗号化されたデータを復号する第３のデータ復号装置を備えた利用者情報収集システムである。

【０００７】請求項４および請求項６に係る発明は、請求項２の発明において、サービス提供者Lとサービス利用者Iとの間で鍵KLIを共有し、サービス利用者Iと前記情報管理者Cとの間で鍵KICを共有し、情報管理者Cと前記サービス提供者Lとの間で鍵KCLを共有し、前記サービス利用者Iは、第１の鍵管理装置において、鍵KLIと鍵KICを管理し、前記情報管理者Cは、第２の鍵管理装置において、鍵KICと鍵KCLを管理し、前記サービス提供者Lは、第３の鍵管理装置において、鍵KCLと鍵KLIを管理し、データの暗号化／復号化には秘密鍵暗号アルゴリズ

7

ムを用いる利用者情報収集システムである。

【０００８】請求項５および請求項７に係る発明は、請求項２の発明において、サービス提供者L、サービス利用者I、情報管理者Cが、それぞれ公開鍵PLと秘密鍵SL、PIとSI、PCとSCを保持し、前記サービス利用者Iは、第１の鍵管理装置において、自身の公開鍵PIと秘密鍵SIを管理し、前記情報管理者Cは、第２の鍵管理装置において、自身の公開鍵PCと秘密鍵SCを管理し、前記サービス提供者Lは、第３の鍵管理装置において、自身の公開鍵PLと秘密鍵SLを管理し、通信相手の公開鍵は、システムに関連するすべての公開鍵を管理する公開鍵管理センタに問い合わせて入手する、もしくは、通信相手の公開鍵を鍵管理装置において管理する構成による利用者情報管理システムである。

【０００９】請求項８に係る発明は、請求項４の発明において、サービス提供者Lとサービス利用者Iとの間でサービスとして授受される情報が、電子的なデータであり、前記サービス提供者Lが提供するサービスにはそれぞれサービス番号SIDが割り当てられており、サービス提供者Lは、サービス送信装置を備え、前記サービス送信装置は、前記サービス番号SIDから、前記鍵管理装置において管理されている前記サービス提供者Lのサービス利用者Iとの共有鍵KLIで提供者署名文SignSIDを生成する署名作成手段を含み、前記サービス番号SIDと前記提供者署名文SignSIDを連結させたSID||SignSIDをサービス利用情報aiとし、サービス利用情報aiを提供するデータに付加して、前記サービス利用者Iに送信する装置であり、前記サービス利用者Iは、サービス受信装置を備え、前記サービス受信装置は、前記サービス利用情報aiを付加したデータを受信すると共に、サービス利用情報aiとサービスデータを分離する装置であり、さらに前記サービス提供者Lは、署名文確認手段を含み、前記署名文確認手段は、前記第３の復号装置において復号されたサービス利用情報aiを、サービス番号SIDと、提供者署名文SignSIDとに分離し、前記サービス番号SIDと提供者署名文SignSIDと、前記サービス提供者Lとサービス利用者Iとの共有鍵KLIによって、前記サービス番号SIDが正しいデータかどうかを確認する手段である構成による利用者情報収集システムである。

【００１０】

【発明の実施の形態】請求項１に係る発明では、サービス提供者Lは、サービス利用者のサービス利用情報aiと、情報管理者が保持するサービス利用者Iの属性情報biを、サービス利用者を特定することなく入手することを可能にする。

【００１１】請求項２に係る発明では、前記情報管理者Cは、前記サービス利用者の識別番号diとこれに対応する前記属性情報biを管理する属性情報管理装置を備え、前記サービス利用者Iは、前記サービス利用者の識別番号diとこれに対応する前記サービス利用情報aiを管理するサービス利用情報管理装置を備え、前記サービス利用者Iは、第1のデータ暗号化装置において、前記サービス利用情報管理装置において管理されている前記サービス利用情報aiを、第1の鍵管理装置において管理されている前記サービス提供者L向けの暗号鍵PILで暗号化して暗号化サービス利用情報E(ai, PIL)を作成し、前記暗号化サービス利用情報E(ai, PIL)と前記識別番号diとを連結したデータE(ai, PIL)||diを、前記第1のデータ暗号化装置において、第1の鍵管理装置において管理されている前記情報管理者C向けの暗号鍵PICで暗号化し、暗号化データE(E(ai, PIL)||di, PIC)を、第1のデータ送受信装置より前記情報管理者Cに向けて送信し、前記情報管理者Cは、前記サービス利用者Iから送信された前記暗号化データE(E(ai, PIL)||di, PIC)を第2のデータ送受信装置において受信し、前記暗号化データE(E(ai, PIL)||di, PIC)を第2のデータ復号化装置において、第2の鍵管理装置において管理されている前記サービス利用者Iからの通信用の前記情報管理者C向けの復号鍵SCIで復号化し、前記暗号化サービス利用情報E(ai, PIL)と前記識別番号diを取り出し、前記属性情報管理装置において、前記識別番号diに対応する属性情報biを読み出し、前記暗号化サービス利用情報E(ai, PIL)と前記属性情報biとを連結したデータE(ai, PIL)||biを作成し、第2のデータ暗号化装置において、前記データE(ai, PIL)||biを、前記第2の鍵管理装置において管理されている前記サービス提供者L向けの暗号鍵PCLで暗号化して暗号化データE(E(ai, PIL)||bi, PCL)を作成し、これを、前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(E(ai, PIL)||bi, PCL)を第3のデータ送受信装置において受信し、これを、第3のデータ復号装置において、第3の鍵管理装置において管理されている前記情報管理者Cからの通信用のサービス提供者Lの復号鍵SLCで復号し、前記暗号化サービス利用情報E(ai, PIL)と前記属性情報biを取り出し、前記暗号化サービス利用情報E(ai, PIL)を、前記第3のデータ復号装置において、前記第3の鍵管理装置おいて管理されている前記サービス利用者Iからの通信用のサービス提供者Lの復号鍵SLIで復号し、サービス利用情報aiを取り出し、前記サービス利用情報aiとそれに対応するサービス利用者Iの属性情報biを、サービス利用者Iを特定することなく得ることを可能にしている。

【００１２】請求項３に係る発明では、前記情報管理者Cは、サービス利用者Iの識別番号diとこれに対応する前記属性情報biを管理する属性情報管理装置を備え、前記サービス提供者Lは、サービス利用者の識別番号diとこれに対して提供したサービス利用情報aiを管理するサービス利用情報管理装置を備え、前記サービス提供者Lは、あるサービス利用情報aiに関連する任意のn人(n ≧ 2)のサービス利用者I1,...,Inに対する識別番号d1,...,dnを連結したデータd1||…||dnを、第3のデータ暗号化

8

9

装置おいて、第3の鍵管理装置において管理されている前記情報提供者C向けの暗号鍵KCによって暗号化して、暗号化データ(d1||…||dn, KC)を作成し、これを前記情報管理者Cに送信し、前記情報管理者Cは、前記サービス提供者Lから送信された前記暗号化データE(d1||…||dn, KC)を受信し、これを第2のデータ復号装置おいて、第2の鍵管理装置において管理されている前記サービス提供者Lからの通信用の前記情報管理者Cの復号鍵DCで復号し、d1||…||dnを取り出し、その内容である、前記識別番号(d1,...,dn)のそれぞれに対応する属性情報(b1,...,bn)を、前記属性情報管理装置において読み出し、不規則な順序に並び変えて結合しb1'||…||bn'を作成し、第2のデータ暗号化装置において、第2の鍵管理装置において管理されている前記サービス提供者L向けの暗号鍵KLによって暗号化して、暗号化データE(b1'||…||bn', KL)を作成し、これを前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(b1'||…||bn', KL)を受信し、これを第3のデータ復号装置おいて、第3の鍵管理装置において管理されている前記情報管理者Cからの通信用の前記サービス提供者Lの復号鍵DLで復号化し、不規則に並び換えられた形態で、前記識別番号d1,...dnのサービス利用者I1,...Inに対する属性情報b1',...bn'を取り出し、これによりサービス利用情報aiとこれに対応するサービス利用者Iの属性情報biを、サービス利用者Iを特定することなく得ることを実現している。

【００１３】請求項４に係る発明では、請求項２の発明に前記サービス提供者Lと前記サービス利用者Iとの間で鍵KLIを共有し、前記サービス利用者Iと前記情報管理者Cとの間で鍵KICを共有し、前記情報管理者Cと前記サービス提供者Lとの間で鍵KCLを共有し、前記サービス利用者Iは、前記サービス利用情報aiを前記共有鍵KLIで暗号化したデータE(ai, KLI)と前記識別番号diの連結を前記共有鍵KICで暗号化したE(E(ai, KLI)||di, KIC)を前記情報管理者Cに送信し、前記情報管理者Cは、前記サービス利用者Iから送信された暗号化データE(E(ai, KLI)||di, KIC)を前記共有鍵KICで復号し、暗号化データE(ai, KLI)と識別番号diを得て、前記識別番号diに対応する前記属性情報biを前記属性管理装置から読み出し、前記属性情報biと暗号化データE(ai, KLI)の連結E(ai, KLI)||biを、前記共有鍵KCLで暗号化し、暗号化データE(E(ai, KLI)||bi, KCL)を前記サービス提供者L送信し、前記サービス提供者Lは、前記情報管理者Cから送信された暗号化データE(E(ai, KLI)||bi,KCL)を前記共有鍵KCLで復号し、E(ai, KLI)とbiを得た後、前記共有鍵KLIでaiを復号することにより、前記サービス利用情報aiとそれに対応するサービス利用者Iの属性情報biを、前記サービス利用情報aiと属性情報biからは、どのサービス利用者Iに関する情報であるかを特定できない状態で得ることを可能にしている。

10

【００１４】請求項５に係る発明は、請求項２の発明において、前記サービス提供者L、前記サービス利用者I、前記情報管理者Cは、それぞれ公開鍵PLと秘密鍵SL、PIとSI、PCとSCを保持し、前記サービス利用者Iは、前記サービス利用情報aiを、前記サービス提供者Lの公開鍵PLで暗号化したサービス利用情報E(ai, PL)を作成し、前記暗号化サービス利用情報E(ai, PL)と前記識別番号diとを連結したデータE(ai, PL)||diを、前記情報管理者Cの公開鍵PCで暗号化し、暗号化データE(E(ai, PL)||di, PC)を、前記データ送受信装置より前記情報管理者Cに向けて送信し、前記情報管理者Cは、前記サービス利用者Iから送信された前記暗号化データE(E(ai,PL)||di, PC)を前記情報管理者Cの秘密鍵SCで復号化し、前記暗号化サービス利用情報E(ai, PL)と前記識別番号diを取り出し、前記属性情報管理装置において、前記識別番号diに対応する前記属性情報biを読み出し、前記暗号化サービス利用情報E(ai, PL)と前記属性情報biとを連結したデータE(ai, PL)||biを、前記サービス提供者Lの公開鍵PLで暗号化したデータE(E(ai, PL)||bi, PL)を作成し、前記暗号化データE(E(ai, PL)||bi), PL)を、前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Iから前記第２のデータ送受信装置より送信された前記暗号化データE(E(ai, PL)||bi,PL)を、前記サービス提供者Lの秘密鍵SLで復号化し、前記暗号化サービス利用情報E(ai, PL)と前記属性情報biを取り出し、前記暗号化サービス利用情報E(ai, PL)を、前記秘密鍵SLで復号化し、サービス利用情報aiを取り出すことにより、前記サービス利用情報aiとそれに対応するサービス利用者Iの属性情報biを、前記サービス利用情報aiと属性情報biからは、どのサービス利用者Iに関する情報であるかを特定できない状態で得ることを可能にしている。

【００１５】請求項６に係る発明は、請求項３の発明において、前記サービス提供者L及び前記情報管理者Cは、共有鍵Kを保持し、前記サービス提供者Lは、あるサービス利用情報aiに関連する任意のn人(n ≧ 2)のサービス利用者I1,...Inに対する識別番号d1,...,dnを連結したデータd1||…||dnを前記共有鍵Kで暗号化したデータE(d1||…||dn, K)を前記情報管理者Cに送信し、前記情報提供者Cは、前記サービス提供者Lから送信された前記暗号化データE(d1||…||dn,k)を前記共有鍵Kで復号化し、前記識別番号(d1,...,dn)のそれぞれに対応する属性情報(b1,...,bn)を、前記属性情報管理装置において読み出し、不規則な順序に並び変えた後に結合してb1'||…||bn'を作成し、前記共有鍵Kで暗号化したデータE(b1'||…||bn', K)を前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(b1'||…||bn', K)を共有鍵Kで復号化し、不規則に並び換えられた形態で、前記識別番号d1,...,dnのサービス利用者I1,...,Inに対する属性情報b1',...,b

11

n'を、利用者Iを特定できな い状態で得ることを実現している。

【００１６】請求項７に係る発明は、請求項３の発明において、前記サービス提供者L、前記情報管理者Cは、それぞれ公開鍵PLと秘密鍵SL、PCとSCを管理し、前記サービス提供者Lは、あるサービス利用情報aiに関連する任意のn人(n ≧ 2)のサービス利用者I1,...,Inに対する識別番号d1,....,dnを連結したデータd1||…||dnを前記情報提供者Cの公開鍵PCで暗号化したデータE(d1||…||dn, PC)を前記情報管理者Cに送信し、前記情報提供者Cは、前記サービス提供者Lから送信された前記暗号化データE(d1||…||dn,PC)を秘密鍵SCで復号化し、前記識別番号(d1,....,dn)のそれぞれに対応する属性情報(b1,....,bn)を、前記属性情報管理装置から読み出し、不規則な順序に並び変えた後に結合してb1'||…||bn'を作成し、前記サービス提供者Lの公開鍵PLで暗号化したデータE(b1'||…||bn', PL)を前記サービス提供者Lに送信し、前記サービス提供者Lは、前記情報管理者Cから送信された前記暗号化データE(b1'||…||bn', PL)を秘密鍵SLで復号化し、不規則に並び換えられた形態で、前記識別番号d1,...dnのサービス利用者I1,...Inに対する属性情報b1',....bn'を、利用者Iを特定できない状態で得ること実現している。

【００１７】請求項８に係る発明では、請求項４の発明において、前記サービス提供者Lと前記サービス利用者Iとの間でサービスとして授受される情報が、電子的なデータであり、前記サービス提供者Lが提供するサービスにはそれぞれサービス番号SIDが割り当てられており、前記サービス提供者Lは、サービス送信装置を備え、前記サービス送信装置は、前記サービス番号SIDから、前記鍵管理装置において管理されている前記サービス提供者Lのサービス利用者Iとの共有鍵KLIで提供者署名文SignSIDを生成する署名作成手段を含み、前記サービス番号SIDと前記提供者署名文SignSIDを連結させたSID||SignSIDをサービス利用情報aiとし、サービス利用情報aiを提供するデータに付加して、前記サービス利用者Iに送信する装置であり、前記サービス利用者Iは、サービス受信装置を備え、前記サービス受信装置は、前記サービス利用情報aiを付加したデータを受信すると共に、サービス利用情報aiとサービスデータを分離する装置であり、さらに前記サービス提供者Lは、署名文確認手段を含み、前記署名文確認手段は、前記第３の復号装置において復号されたサービス利用情報aiを、サービス番号SIDと、提供者署名文SignSIDとに分離し、前記サービス番号SIDと提供者署名文SignSIDと、前記サービス提供者Lとサービス利用者Iとの共有鍵KLIによって、前記サービス番号SIDが正しいデータかどうかを確認する手段であり、これによって、サービス提供者Lが、サービス利用者Iを特定することなく、サービス提供者Lの提供するサービス利用情報aiと、そのサービスを利用したサービス

12

利用者の利用者属性情報biとを入手できるのみでなく、サービス提供者Lが、受信したサービス利用情報aiの正当性を検証できることを可能にしている。

【００１８】（実施の形態１）図1は本発明の一実施の形態に係る利用者情報収集システムの基本構成を示すブロック図である。

【００１９】図1において、本実施の形態における利用者情報収集システムは、サービス提供者Lとサービス利用者I、サービス利用者Iに関する情報を保持している情報管理者Cから構成される。サービス提供者L、サービス利用者I、情報管理者Cには、それぞれデータ送受信装置10、20、30と、データ暗号化／復号化装置11、21、31と、鍵管理装置12、22、32が備えられており、情報提供者Cとサービス提供者Lとの間およびサービス利用者Iと情報提供者Cとの間は通信路40および通信路41で結ばれており双方向に情報をやりとりする。情報管理者Cは、サービス利用者Iに関する属性情報biとサービス利用者Iの識別番号diを管理する、属性情報管理装置33を備えており、サービス利用者Iは、サービス利用情報aiと上記識別番号diを管理する、サービス利用情報管理装置23を備えている。情報管理者Cには、ネットワーク上での一意な識別子ネットークIDが付与されているとする。

【００２０】図２は、本発明の一実施の形態に係るサービス提供者Lの基本構成を示す図である。図２において、サービス提供者Lの基本構成を説明すると、データ送受信装置10は、通信路40を通じて情報管理者Cとの間でやりとりされるデータの送信及び受信を行なう装置である。鍵管理装置12は、鍵記憶装置120と鍵読み出し装置121から構成される。鍵記憶装置120には、電子的なデータからなる鍵が格納されており、格納されている鍵は、鍵読み出し装置121からのみ読み出すことが可能で、外部から読みだすことは出来ない。データ暗号化／復号化装置11は、電子的なデータを暗号化あるいは復号する装置であり、データ処理部110とプログラム格納装置111から構成される。プログラム格納装置111には暗号化及び復号化を行なうプログラムが格納されている。データ処理部110は、このプログラムによって動作し、データ入出力装置10から入力されるデータを、鍵読み出し装置121から読み出された鍵によって、暗号化または復号する。

【００２１】図３は、本発明の一実施の形態におけるサービス利用者Iの基本構成を示す図である。図３において、サービス提供者Iの基本構成を説明すると、データ送受信装置20は、通信路41を通じて情報管理者Cとの間でやりとりされるデータの送信及び受信を行なう装置である。鍵管理装置22は、鍵記憶装置220と鍵読み出し装置221から構成される。鍵記憶装置220には、電子的なデータからなる鍵が格納されており、格納されている鍵は、鍵読み出し装置221からのみ読み出すことが可能で、外部から読みだすことは出来ない。サービス利用情

13

報管理装置23は、サービス利用情報記憶装置230とサービス利用情報入出力装置231から構成されている。サービス利用情報記憶装置230には、サービス利用情報aiとサービス利用者識別番号diが格納されており、データの読み出し及び書き込みは、サービス利用情報入出力装置231からのみ行なうことが出来、外部からの読み出し及び書き込みは出来ない。データ暗号化／復号化装置21は、電子的なデータを暗号化あるいは復号する装置であり、データ処理部210とプログラム格納装置211から構成される。プログラム格納装置211には暗号化及び復号化を行なうプログラムが格納されている。データ処理装置210は、このプログラムによって動作し、鍵読み出し装置221から読み出された鍵によって、データ入出力装置20から入力されるデータを復号する処理と、鍵読み出し装置221から読み出された鍵によって、サービス利用情報入出力装置231から読み出したデータを暗号化し、データ入出力装置20に送る処理を行なう。

【００２２】図４は、本発明の一実施の形態における情報提供者Cの基本構成を示す図である。図４において、情報提供者Cの基本構成を説明すると、データ送受信装置30は、通信路40を通じてサービス提供者Lとの間で、通信路41を通じてサービス利用者Iとの間でやりとりされるデータの送信及び受信を行なう装置である。鍵管理装置32は、鍵記憶装置320と鍵読み出し装置321から構成される。鍵記憶装置320には、電子的なデータからなる鍵が格納されており、格納されている鍵は、鍵読み出し装置321からのみ読み出すことが可能で、外部から読みだすことは出来ない。属性情報管理装置33は、属性情報記憶装置330と属性情報入出力装置331から構成されている。属性情報記憶装置330には、サービス利用者識別番号diとサービス利用者Iの属性情報biが格納されており、データの読み出し及び書き込みは、属性情報入出力装置331からのみ行なうことが出来、外部からの読み出し及び書き込みは出来ない。データ暗号化／復号化装置31は、電子的なデータを暗号化あるいは復号する装置であり、データ処理部310とプログラム格納装置311から構成される。プログラム格納装置311には暗号化及び復号化を行なうプログラムが格納されている。

【００２３】データ処理部310は、このプログラムによって動作し、鍵読み出し装置321から読み出された鍵によって、データ入出力装置30から入力されるデータを復号する処理と、鍵読み出し装置321から読み出された鍵によって、サービス利用情報入出力装置31から読み出したデータを暗号化し、データ入出力装置30に送る処理を行なう。

【００２４】また、本発明の一実施の形態において、各サービス利用者Iは、サービス提供者Lが提供するサービスに加入する前に、クレジット会社に入会しており、各サービス利用者Iには、クレジット番号が与えられており、クレジット会社には、サービス利用者の年収、学

14

歴、職業等極めてプライベートな個人情報が保持されている。本発明の一実施の形態おいては、クレジット会社を情報管理者C、クレジット番号をサービス利用者識別子di、個人情報を属性情報biとする。サービス利用者Iは、サービス提供者Lの提供するサービスを利用する。本実施の形態では、サービスとしてケーブルテレビ放送等通信路によってデータが送信される場合を考える。すなわち、図５で示すように、サービス提供者Lは、サービス送信装置50を備え、サービス利用者Iは、サービス受信装置51を備え、サービスは、サービス送信装置50から通信路52を経由してサービス受信装置51において受信される。サービス受信装置51には、サービス利用情報収集装置510があり、サービスプログラムの内容やサービス利用時間等サービス利用者Iのサービス利用情報aiを収集し、収集したサービス利用情報aiは、図３に示すサービス利用情報管理装置23で管理される。

【００２５】また、本発明の一実施の形態おいては、サービス提供者Lは、サービス送信装置50から、定期的にサービス利用情報送信要求を、サービス利用者Iに送信し、サービス受信装置51において、サービス利用情報送信要求を受信したIは、図６～９に示す動作を行なう。図６は、図1に示す利用者情報収集システムの全体の動作を示すシーケンスチャートである。図7は、図1のサービス利用者Iの、サービス利用情報ai送信時の動作を示すフローチャートである。図8は、図1の情報管理者Cの、属性情報bi送信時の動作を示すフローチャートである。図9は、図1のサービス提供者Lの、属性情報bi受信時の動作を示すフローチャートである。

【００２６】以下、これら図6～図9を参照して、本実施の形態の動作を説明する。サービス利用者Iには、公開鍵暗号アルゴリズムEと、サービス提供者Lおよび情報提供者Cの公開鍵PL及びPCを配布し、情報管理者Cには、公開鍵暗号アルゴリズムEおよび公開鍵復号アルゴリズムDと、サービス提供者Lの公開鍵PLおよび自らの秘密鍵SCを配布し、サービス提供者Lには、公開鍵復号アルゴリズムDと、自らの秘密鍵SLを配布する。

【００２７】このとき、y(yは、C、Lのうちのいずれか）の公開鍵Pyを用いて公開鍵暗号アルゴリズムEによりデータXを暗号化したデータE(X, Py)を復号できるのは、公開復号アルゴリズムDと秘密鍵Syを保持しているものに限られる。すなわち、

$$X = D(E(X, Py), Sy)$$

が成立する。また、秘密鍵Syは、yしか知らない。また、公開鍵Pyから対応する秘密鍵Syを類推することは出来ない。サービス利用者I、情報管理者Cには、公開鍵暗号アルゴリズムEが配布され、それぞれのデータ暗号化／復号化装置11、21、31内のプログラム格納装置111、211、311に格納されている。

【００２８】なお、公開鍵アルゴリズムに関しては、「現代暗号理論」池野信一・小山謙二著（電気情報通信

15

学会）に詳しく述べられているので参照されたい。

【００２９】サービス利用者Iは、サービス利用時に利用したサービスの内容を示すサービス利用情報aiを、サービス利用情報管理装置23に格納する。サービス利用者Iは、定期的にサービス情報管理装置23よりサービス利用情報aiを読み出す（図7のステップS101）。

【００３０】また、サービス提供者Lの公開鍵PLを、鍵管理装置22より読み出す（ステップS102）。

【００３１】次に、データ暗号化／復号化装置21において、プログラム格納装置211に格納した公開鍵暗号アルゴリズムEをデータ処理部210に読み込み、読み出した公開鍵PLで、サービス利用情報aiを(1)式のように暗号化する（ステップS103）。

【００３２】E(ai, PL)　　……(1)

続いて、送信先の情報提供者Cの公開鍵PCを鍵管理装置22から読み出す（ステップS104）。

【００３３】さらに、サービス利用者Iの識別番号diを、サービス利用情報管理装置23より読み出し（ステップS105）、(1)式の暗号化サービス利用情報E(ai, PL)と連結する（ステップS106）。その後、データ暗号化／復

D(E(E(ai, PL)||di, PC), SC) = E(ai, PL)||di　　……(3)

続いて、情報管理者Cは、識別番号diに対応する属性情報biを、属性情報管理装置33から読み出し（ステップS204）、属性情報biと暗号化サービス利用情報E(ai, PL)を連結する（ステップS205）。

【００３９】また、サービス提供者Lの公開鍵PLを、鍵管理装置32より読み出し（ステップS206）、データ復号化／暗号化装置31において、プログラム格納装置311に格納されている公開鍵暗号アルゴリズムEを、データ処理部310に読み出し、公開鍵PLで、連結データE(ai, PL)||biを(4)式のように暗号化する（ステップS207）。

【００４０】E(E(ai, PL)||bi, PL)　　……(4)

最後に、暗号化データE(E(ai, PL)||bi, PL)をデータ入出力装置30より、通信路40を用いて、サービス提供者Lに送信する（図６のメッセージ２に対応）。

D(E(E(ai, PL)||bi, PL), SL) = E(ai, PL)||bi　　……(5)

さらに、暗号化サービス利用情報E(ai, PL)を、秘密鍵SLで(6)式のように復号し、サービス利用情報aiを取り出す。

【００４５】D(E(ai, PL), SL) = ai　　……(6)

この時点で、サービス提供者Lは、サービス利用者Iのサービス利用情報aiと、情報管理者Cが管理するサービス利用者Iの属性情報biとを入手することが出来るが、サービス提供者Lは、入手したサービス利用情報aiと属性情報biから、この情報がどのサービス利用者に関するものであるかを特定することは出来ない。

【００４６】本実施の形態により、サービス提供者Lは、従来入手出来なかったサービス利用者Iの属性情報biを入手することが可能である。また、情報管理者Cは、既存の属性情報biを有効に利用することが出来、サービス利用者Iのプライバシーの問題も解決される。また、データを暗号化することにより、データの盗聴などに対して安全に通信することが出来る。

16

＊号化装置21において読み出したPCで、連結したデータE(ai, PL)||diを(2)式のように暗号化する（ステップS107）。

【００３４】E(E(ai, PL)||di, PC)　　……(2)

ただし、||は情報の連結を表す。暗号化したデータE(E(ai, PL)||di, PC)を情報管理者Cに送信する（ステップS108、図６のメッセージ１に対応）。

【００３５】情報管理者Cは、通信路41を用いてサービス利用者Iから送信された暗号化データE(E(ai, PL)||di, PC)をデータ送受信装置30において受信する（ステップS201）。

【００３６】次に、情報管理者Cは、自分の秘密鍵SCを鍵管理装置32から読み出す（ステップS202）。

【００３７】次に、データ暗号化／復号化装置31において、データ処理装置310に、プログラム格納装置311に格納されている公開鍵復号アルゴリズムDを読み出し、秘密鍵SCで、暗号化データE(E(ai, PL)||di, PC)を(3)式のように復号し、E(ai,PL)||diを取り出す（ステップS203）。

【００３８】

※【００４１】サービス提供者Lは、通信路40を用いて情報管理者Cから送信された暗号化データE(E(ai, PL)||bi, PL)をデータ送受信装置10において受信する（図9のステップS301）。

【００４２】次に、サービス提供者Lは、自分の秘密鍵SLを鍵管理装置12から読み出す（ステップS302）。

【００４３】次に、データ暗号化／復号装置11において、データ処理部110に、プログラム格納装置111に格納されている公開鍵復号アルゴリズムDを読み出し、秘密鍵SLで、暗号化データE(E(ai, PL)||bi, PL)を(5)式のように復号し、E(ai,PL)||biを取り出す（ステップS303）。

【００４４】

【００４７】なお、上記実施の形態において、ある秘密鍵暗号アルゴリズムFと秘密鍵復号アルゴリズムF^{-1}において、鍵Kを用いて秘密鍵暗号アルゴリズムFによりデータXを暗号化した関数F(X, K)を復号できるのは、秘密鍵復号アルゴリズムと鍵Kの双方を保持しているものに限られる。すなわち、

$X = F^{-1}(F(X, K), K)$　　……(7)

が成立する場合、公開鍵暗号アルゴリズムEおよび公開鍵復号アルゴリズムDの代わりに秘密鍵暗号アルゴリズムFと秘密鍵復号アルゴリズムF^{-1}をプログラム格納装置111、211、311に格納し、サービス利用者Iと情報管理者

17

Cとの共有鍵KICを鍵管理装置22、32に格納し、情報管理者Cとサービス提供者Lとの共有鍵KCLを鍵管理装置12、32に格納し、サービス提供者Lとサービス利用者Iとの共有鍵KLIを鍵管理装置12、22に格納し、サービス利用者Iにおいて、サービス利用情報aiの暗号化を、共有鍵KLIを用いた秘密鍵暗号アルゴリズムFによって行ない、暗号化サービス利用情報をF(ai, KLI)とし、暗号化サービス利用情報と識別番号diとの連結データをF(ai, KLI)||di とし、連結データF(ai, KLI)||diを、共有鍵KICを用いて、秘密鍵暗号化アルゴリズムFを用いて暗号化し、暗号化データをF(F(ai,KLI)||di, KIC)として、情報提供者Cに送信し、情報提供者Cは、受信した暗号化データF(F(ai, KLI)||di, KIC)を共有鍵KICを用いて秘密鍵復号アルゴリズムF^{-1}によって復号し、暗号化サービス利用情報F(ai, KLI)と属性情報biを連結させたデータを共有鍵KCLと秘密鍵暗号アルゴリズムFによって暗号化し、F(F(ai, KLI)||bi, KCL)を暗号化データとしてサービス提供者Lに送信し、サービス提供者Lは、受信した暗号化データF(F(ai, KLI)||bi, KCL)を共有鍵KCLを用いて秘密鍵復号アルゴリズムF^{-1}によって復号し、暗号化サービス利用情報F(ai, KLI)と属性情報biを取り出し、暗号化サービス利用情報F(ai, KLI)を共有鍵KLIを用いて秘密鍵復号アルゴリズムF(-1)によって復号し、サービス利用情報aiを取り出すことによっても同様の効果が得られる。

【００４８】また、上記実施の形態において、あるデータXに対してある秘密鍵SKeyを用いて電子署名Signを施す、署名生成アルゴリズムSと、対応する公開鍵PKeyを用いて電子署名Signが、秘密鍵Skeyを保持する者が作成したデータXに対する電子署名であるかどうかを確認できる、署名確認アルゴリズムVがあり、署名生成アルゴリズムSを、サービス利用者I及び情報提供者Cのプログラム格納装置211、311に格納し、署名確認アルゴリズムを、情報管理者Cおよびサービス提供者Lのプログラム格納装置311、111に格納し、サービス利用者Iは、公開鍵PIに対応した秘密鍵SIを鍵記憶装置220に格納し、サービス提供者Lは、情報提供者Cの公開鍵PCを鍵記憶装置120に格納する場合、サービス利用者Iにおいて、暗号化サービス利用情報E(ai, PL)と識別番号diを連結したデータE(ai, PL)||diに、秘密鍵SIを用いて、署名生成アルゴリズムSによって電子署名SignICを作成し、暗号化データE(E(ai, PL)||di, PC)と共に情報管理者Cに送信し、情報管理者Cにおいて、サービス利用者Iの公開鍵PIと署名確認アルゴリズムVによって、受信した電子署名SignICが、サービス利用者Iが、データE(ai,PL)||diに対して施した電子署名であることを確認し、また、情報管理者Cにおいて、暗号化サービス利用情報E(ai, PL)と属性番号biを連結したデータE(ai, PL)||biに、秘密鍵SCを用いて、署名生成アルゴリズムSによって電子署名SignCLを作成し、暗号化データE(E(ai, PL)||bi, PL)と共

18

にサービス提供者Lに送信し、サービス提供者Lにおいて、情報管理者Cの公開鍵PCと署名確認アルゴリズムVによって、受信した電子署名SignCLが、情報管理者Cが、データE(ai, PL)||biに対して施した電子署名であることを確認するように実現した場合、上記実施の形態に示した効果の他に、受信したデータが正しいかどうか確認することが出来、第三者によるデータの改竄を防ぐことが可能になる。

【００４９】また、上記実施の形態において、サービス提供者Lのプログラム格納装置111に、署名生成アルゴリズムSを格納し、サービス提供者Lが、提供するサービス内容を識別出来る、サービス番号SIDを各サービスに一意に割り当て、サービス提供者Lにおいて、サービス番号SIDに、サービス提供者Lの秘密鍵SLを用いて、署名生成アルゴリズムSによって電子署名SignSIDを作成し、電子署名SignSIDとサービス番号SIDとを連結したデータSignSID||SIDをサービス利用情報aiとして、サービスするデータに付加して送信し、サービス利用情報aiを付加されたサービスを受信したサービス利用者Iは、サービス利用情報510においてサービス番号SIDを取り出し、サービス利用情報管理装置23において管理し、以下、上記実施の形態の図6～図8に示した動作で、サービス提供者LにE(E(ai, PL)||bi, PL)を送信する。

【００５０】暗号化データE(E(ai, PL)||bi, PL)を受信したサービス提供者Lは、図9に示した動作で、サービス利用情報aiと属性情報biを取り出し、取り出したサービス利用情報aiを、電子署名SignSIDとサービス番号SIDに分離し、サービス利用情報aiに、サービス提供者Lの秘密鍵SLと、署名生成アルゴリズムSによって、新たに生成した電子署名SignSID'と受信した電子署名SignSIDとを比較することによって、受信したサービス利用情報の正しさを検証出来る様に実現した場合、上記実施の形態に示した効果の他に、第三者によるサービス利用情報aiの改竄を防ぐことが可能になる。

【００５１】（実施の形態２）図10は本発明の一実施の形態に係る利用者情報収集システムの基本構成を示すブロック図である。図10において、本実施の形態における利用者情報収集システムは、サービス提供者Lとサービス利用者I、サービス利用者Iに関する情報を保持している情報管理者Cから構成される。サービス提供者L、サービス利用者I、情報管理者Cには、それぞれデータ送受信装置10、20、30と、データ暗号化／復号化装置11、21、31と、鍵管理装置12、22、32が備えられており、情報管理者Cとサービス提供者Lとの間は通信路40で結ばれており双方向に情報をやりとりする。情報管理者Cは、サービス利用者Iに関する属性情報biとサービス利用者Iの識別番号diを管理する、属性情報管理装置33を備えており、サービス提供者Lは、サービス利用者Iのサービス利用情報aiとサービス利用者Iの識別番号diを管理する、サービス利用情報管理装置13を備えている。

19

【００５２】図11は、本発明の一実施の形態に係るサービス提供者Lの基本構成を示す図である。図11において、サービス提供者Lの基本構成を説明すると、データ送受信装置10は、通信路40を通じて情報管理者Cとの間でやりとりされるデータの送信及び受信を行なう装置である。データ暗号化／復号化装置11は、電子的なデータを暗号化あるいは復号する装置であり、データ処理部110とプログラム格納装置111から構成される。鍵管理装置12は、鍵記憶装置120と鍵読み出し装置121から構成される。鍵記憶装置120には、電子的なデータからなる鍵が格納されており、格納されている鍵は、鍵読み出し装置121からのみ読み出すことが可能で、外部から読みだすことは出来ない。サービス利用情報管理装置13は、サービス利用情報記憶装置130とサービス利用情報入出力装置131から構成されている。サービス利用情報記憶装置130には、サービス利用情報aiとサービス利用者Iの識別番号diが格納されており、データの読み出し及び書き込みは、サービス利用情報入出力装置131からのみ行なうことが出来、外部からの読み出し及び書き込みは出来ない。プログラム格納装置111には暗号化及び復号化を行なうプログラムが格納されている。データ処理部110は、このプログラムによって動作し、データ入出力装置10から入力されるデータを、鍵読み出し装置121から読み出された鍵によって、復号する処理と、鍵読み出し装置121から読み出された鍵によって、サービス利用情報入出力装置13から読み出したデータを暗号化し、データ入出力装置30に送る処理を行なう。

【００５３】本実施の形態２における、サービス利用者Iおよび情報管理者Cの構成は、実施の形態１において図3と図4で示した構成と同じである。

【００５４】また、本発明の一実施の形態において、各サービス利用者Iは、サービス提供者Lが提供するサービスに加入する前に、クレジット会社に入会しており、各サービス利用者Iには、クレジット番号が与えられており、クレジット会社には、サービス利用者の年収、学歴、職業等極めてプライベートな個人情報が保持されている。本発明の一実施の形態おいては、クレジット会社を情報管理者C、クレジット番号をサービス利用者Iの識別番号di、個人情報を属性情報biとする。サービス利用者Iは、サービス提供者Sの提供するサービスを利用する。本実施の形態では、サービスとしてケーブルテレビ放送等通信路によってデータが送信される場合を考える。すなわち、図５で示すように、サービス提供者Lは、サービス送信装置50を備え、サービス利用者Iは、サービス受信装置51を備え、サービスは、サービス送信装置50から通信路53を経由してサービス受信装置51において受信される。

【００５５】また、本発明の一実施の形態おいて、サービス提供者Lは、サービス利用情報aiに関連するサービス利用者Iに関する属性情報biを入手する際、図12～15

20

に示す動作を行なう。図12は、図10に示す利用者情報収集システムの全体の動作を示すシーケンスチャートである。図13は、図10のサービス提供者Lの、識別番号di送信時の動作を示すフローチャートである。図14は、図10の情報管理者Cの、識別番号di受信時の動作を示すフローチャートである。図15は、図10のサービス提供者Lの、属性情報bi受信時の動作を示すフローチャートである。

【００５６】以下、これら図12～図15を参照して、本実施の形態の動作を説明する。情報管理者Cには、公開鍵暗号アルゴリズムEおよび公開鍵復号アルゴリズムDと、サービス提供者Lの公開鍵PLおよび自らの公開鍵PCと秘密鍵SCを配布し、サービス提供者Lには、公開鍵暗号アルゴリズムEおよび公開鍵復号アルゴリズムDと、情報管理者Cの公開鍵PCおよび自らの公開鍵PLと秘密鍵SLとを配布する。このとき、y(yは、C、Lのうちのいずれか)の公開鍵Pyを用いて公開鍵暗号アルゴリズムEにより,データXを暗号化した関数E(X, Py)を復号できるのは、公開復号アルゴリズムDと秘密鍵Syを保持しているものに限られる。すなわち、

$$X = D(E(X, Py), Sy) \quad \cdots\cdots (8)$$

が成立する。また、秘密鍵Syは、yしか知らない。また、公開鍵Pyから対応する秘密鍵Syを類推することは出来ない。サービス提供者L、情報管理者Cには、公開鍵暗号アルゴリズムE、および公開鍵復号アルゴリズムDが配布され、それぞれのデータ暗号化／復号化装置11、31内のプログラム格納装置111、311に格納されている。

【００５７】サービス提供者Lは、サービス利用者Iのサービス利用情報aiを、サービス利用情報管理装置13において管理している。サービス提供者Lは、サービス利用情報aiに関するn人($n \geqq 2$)のサービス利用者I1,....,Inに関する属性情報を入手したい場合、サービス提供者Lは、サービス利用情報aiに関連するサービス利用者の識別番号diを、サービス利用情報管理装置13より読み出し、読み出した識別番号d1,....,dnを連結し、連結データd1||…||dnを作成する(図13のステップS401)。

【００５８】続いて、情報管理者Cの公開鍵PCを、鍵管理装置12より読み出す（ステップS402）。

【００５９】サービス提供者Lは、データ暗号化／復号化装置11において、プログラム格納装置111に格納した公開鍵暗号アルゴリズムEをデータ処理部110に読み込み、読み出した公開鍵PCで、連結データd1||…||dnを式(9)のように暗号化し、暗号化したデータE(d1||…||dn, PC)を情報管理者Cに送信する（ステップS403、及び図１２のメッセージ１に対応）。

【００６０】$$E(d1||\cdots||dn, PC) \quad \cdots\cdots (9)$$

情報管理者Cは、通信路40を用いてサービス提供者Lから送信された暗号化データE(d1||…||dn, PC)をデータ送受信装置30において受信する（図14のステップS501）。

【００６１】次に、情報管理者Cは、自分の秘密鍵SCを

21

鍵管理装置32から読み出す（ステップS502）。

【００６２】次に、データ暗号化／復号装置31において、データ処理部310に、プログラム格納装置311に格納されている公開鍵復号アルゴリズムDを読み出し、秘密＊

$$D(E(d1||\cdots||dn,\ SC) = d1||\cdots||dn \quad \cdots\cdots\cdots (10)$$

続いて、情報管理者Cは、取り出した識別番号d1,....,dnに対応する属性情報b1,....,bnを、属性情報管理装置33から読み出す（ステップS504）。

【００６４】その後、b1,....,bnを不規則な順序に並べ換えて結合し、結合データb1'||…||bn'を作成する（ステップS505）。

【００６５】さらに、情報管理者Cは、サービス提供者Lの公開鍵PLを、鍵管理装置32より読み出し（ステップS506）、データ復号化／暗号化装置31において、プログラム格納装置311に格納されている公開鍵暗号アルゴリズムEを、データ処理部310に読み出し、公開鍵PLで、連結データb1'||…||bn'を(11)式のように暗号化し、暗号化したデータE(b1'||…||bn', PL)をサービス管理者Lに送信する（ステップS507、及び図１２のメッセージ２に対応）。

※20

$$D(E(b1'||\cdots||bn',\ SL) = b1'||\cdots||bn' \quad \cdots\cdots\cdots (12)$$

この時点で、サービス提供者Lは、あるサービス利用情報aiに関するサービス利用者I1,....Inの属性情報b1',....bn'を入手することが出来るが、サービス提供者Lは、入手した属性情報b1',....,bn'の任意のbkについて、この情報がどのサービス利用者に関するものであるかを特定することは出来ない。

【００７０】本実施の形態により、サービス提供者Lは、従来入手出来なかったサービス利用者Iの属性情報biを入手することが可能である。また、情報管理者Cは、既存の属性情報biを有効に利用することが出来、サービス利用者Iのプライベートの問題も解決される。また、データを暗号化することにより、データの盗聴などに対して安全に通信することが出来る。全体の通信回数も小さくて済む。

【００７１】なお、上記実施の形態において、ある秘密鍵暗号アルゴリズムFと秘密鍵復号アルゴリズムF^{-1}において、鍵Kを用いて秘密鍵暗号アルゴリズムFによりデータXを暗号化した関数F(X, K)を復号できるのは、秘密鍵★

$$F^{-1}(F(d1||\cdots||dn,\ KCL),\ KCL) = d1||\cdots||dn \quad \cdots\cdots\cdots (15)$$

続いて、連結データb1'||…||bn'の暗号化を、共有鍵KCLと秘密鍵暗号アルゴリズムFによって(16)式の様に暗号化し、暗号化したデータをサービス提供者Lに送信する。

【００７２】F(b1'||…||bn', KCL)　……(16)

さらに、サービス提供者Lにおいて、受信した暗号化データF(b1'||…||bn', KCL)を共有鍵KCLを用いて秘密鍵復号アルゴリズムF^{-1}によって復号し、連結データb1'||…||bn'を取り出す様に実現した場合でも、同様の効果が得られる。

22

＊鍵SCで、暗号化データE(d1||…||dn, PC)を(10)式のように復号し、連結データd1||…||dnを取り出す（ステップS503）。

【００６３】

※【００６６】E(b1'||…||bn', PL)　……(11)

サービス提供者Lは、通信路40を用いて情報管理者Cから送信された暗号化データE(b1'||…||bn', PL)をデータ送受信装置10において受信する（図15のステップS601）。

【００６７】次に、サービス提供者Lは、自分の秘密鍵SLを鍵管理装置12から読み出す（ステップS602）。

【００６８】次に、データ暗号化／復号装置11において、データ処理部110に、プログラム格納装置111に格納されている公開鍵復号アルゴリズムDを読み出し、秘密鍵SLで、暗号化データE(b1'||…||bn', PL)を(12)式のように復号し、b1',....,bn'を取り出す（ステップS603）。

【００６９】

★復号アルゴリズムと鍵Kの双方を保持しているものに限られる、すなわち、

$$X = F^{-1}(F(X,\ K),\ K) \quad \cdots\cdots\cdots (13)$$

が成立する場合、公開鍵暗号アルゴリズムEおよび公開鍵復号アルゴリズムDの替わりに秘密鍵暗号アルゴリズムFと秘密鍵復号アルゴリズムF^{-1}をプログラム格納装置111、311に格納し、情報管理者Cとサービス提供者Lとの共有鍵KCLを鍵管理装置12、32に格納し、サービス提供者Lにおいて、連結データd1||…||dnの暗号化を、共有鍵KCLを用いた秘密鍵暗号アルゴリズムFによって(14)式のように行ない、暗号化したデータを情報管理者Cに送信し、

F(d1||…||dn, KCL)　……(14)

情報提供者Cにおいて、受信した暗号化データF(d1||…||dn, KCL)を共有鍵KCLを用いて秘密鍵復号アルゴリズムF^{-1}によって(15)式のようにして復号して、連結データd1||…||dnを取り出し、

【００７３】

【発明の効果】以上説明したように、請求項１によれば、サービス提供者Lは、サービス利用者のサービス利用情報aiと、従来は得ることができなかった情報管理者が保持するサービス利用者Iの属性情報biを、サービス利用者Iを特定することなく入手することが出来る。

【００７４】請求項２の発明によれば、サービス利用者Iは、サービス提供者L向けにサービス利用情報を暗号化し、暗号化されたサービス利用情報に利用者Iの識別情報diを連結させて、情報管理者C向けに暗号化して、情

報管理者Cに送信する。情報管理者Cは、識別情報diを取り出すことが出来、サービス利用情報aiは暗号化されたままで、見ることは出来ない。情報管理者Cは、識別情報diに対応する属性情報biを取り出し、この属性情報biと、暗号化されたサービス利用情報aiとを合わせて、サービス提供者L向けに暗号化し、サービス提供者Lに送信する。サービス利用情報ai及び属性情報biは、サービス提供者Lのみが復号でき、サービス提供者Lは、サービス利用情報aiと属性情報biを入手することが出来るが、入手した、サービス利用情報aiと属性情報biには、サービス利用者Iを識別する情報は含まれていないため、サービス提供者Lは、サービス利用情報aiと属性情報biから、これらの情報に関連するサービス利用者Iを特定することは出来ない。データの暗号化及び復号化には、公開鍵暗号アルゴリズムおよび秘密鍵暗号アルゴリズムのどちらも用いることが出来る。

【００７５】請求項３に示す発明によれば、サービス提供者Lにおいて、あるサービス利用情報aiに関連するn人($n \geqq 2$)の識別番号d1, d2, …, dnを連結し、情報管理者Cに向けて暗号化を行ない、暗号化したデータを情報管理者Cに送信し、情報管理者Cは、サービス提供者Lから送信された暗号化データを復号することにより、n人の識別番号d1, d2, …, dnを得、対応するn人の属性情報b1, b2, …, bnを取り出し、不規則な順序に並び換えて連結し、サービス提供者向けに暗号化し、さらに、サービス提供者Lは、情報管理者Cから送信された暗号化データを復号することによりn個の属性情報が得られるが、得られた任意の属性情報bk($1 \leqq k \leqq n$)からは、当該属性情報がどのサービス利用者に関する情報であるのかを特定できない。

【００７６】請求項８に係る発明によれば、サービス提供者Lとサービス利用者Iとの間でサービスとして授受される情報が、電子的なデータであり、前記サービス提供者Lが提供するサービスにはそれぞれサービス番号SIDが割り当てられている場合に、前記サービス提供者Lは、前記サービス番号SIDから、前記鍵管理装置において管理されている前記サービス提供者Lのサービス利用者Iとの共有鍵KLIで提供者署名文SignSIDを生成し、前記サービス番号SIDと前記提供者署名文SignSIDを連結させたSID||SignSIDをサービス利用情報aiとし、サービス利用情報aiを提供するデータに付加して、前記サービス利用者Iに送信し、さらに前記サービス提供者Lは、署名文確認手段を含み、復号装置において復号されたサービス利用情報aiを、サービス番号SIDと、提供者署名文SignSIDとに分離し、前記サービス番号SIDと提供者署名文SignSIDと、前記サービス提供者Lとサービス利用者Iとの共有鍵KLIによって、前記サービス番号SIDが正しいデータかどうかを確認することにより、サービス提供者Lが、サービス利用者Iを特定することなく、サービス提供者Lの提

供するサービス利用情報aiと、そのサービスを利用したサービス利用者の利用者属性情報biとを入手できるのみでなく、サービス提供者Lが、受信したサービス利用情報aiの正当性を検証できることを可能にしている。

【図面の簡単な説明】

【図１】本発明の実施の形態１の主要構成を示す図

【図２】本発明の実施の形態１におけるサービス提供者Lの構成を示す図

【図３】本発明の実施の形態１におけるサービス利用者Iの構成を示す図

【図４】本発明の実施の形態１における情報管理者Cの構成を示す図

【図５】本発明の実施の形態１におけるサービス提供者Lとサービス利用者Iとの間のサービスの提供及び利用形態を示す図

【図６】本発明の実施の形態１における通信メッセージのシーケンスを示す図

【図７】本発明の実施の形態１におけるサービス利用者Iが行う処理の流れ図

【図８】本発明の実施の形態１における情報管理者Cが行う処理の流れ図

【図９】本発明の実施の形態１におけるサービス提供者Lが行う処理の流れ図

【図１０】本発明の実施の形態２の主要構成を示す図

【図１１】本発明の実施の形態２におけるサービス提供者Lの構成を示す図

【図１２】本発明の実施の形態２における通信メッセージのシーケンスを示す図

【図１３】本発明の実施の形態２におけるサービス提供者Lがデータ送信時に行う処理の流れ図

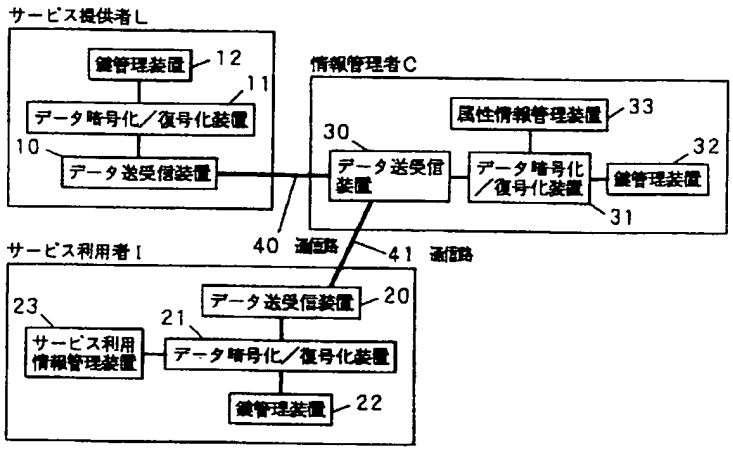
【図１４】本発明の実施の形態２における情報管理者Cが行う処理の流れ図

【図１５】本発明の実施の形態２におけるサービス提供者Lがデータ受信時に行う処理の流れ図

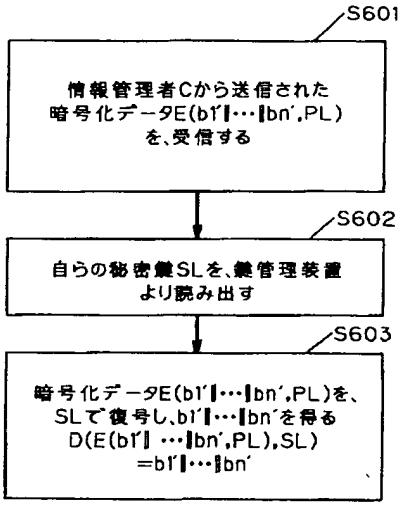
【符号の説明】

１０　サービス提供者Lのデータ送受信装置
１１　サービス提供者Lのデータ暗号化／復号化装置
１２　サービス提供者Lの鍵管理装置
２０　サービス利用者Iのデータ送受信装置
２１　サービス利用者Iのデータ暗号化／復号化装置
２２　サービス利用者Iの鍵管理装置
２３　サービス利用者Iのサービス利用情報管理装置
３０　情報管理者Cのデータ送受信装置
３１　情報管理者Cのデータ暗号化／復号化装置
３２　情報管理者Cの鍵管理装置
３３　情報管理者Cの属性情報管理装置
５０　サービス提供者Lのサービス送信装置
５１　サービス利用者Iのサービス受信装置

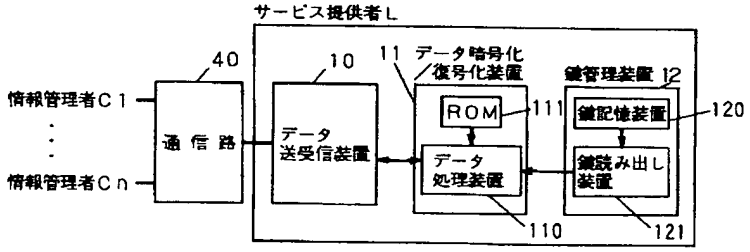
【図１】



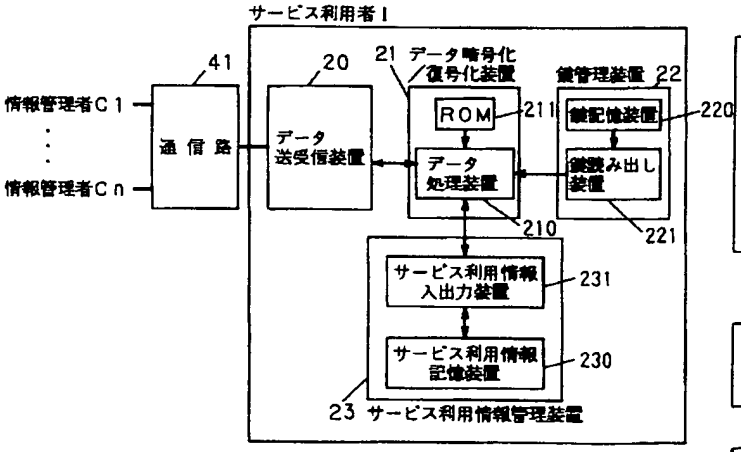
【図１５】



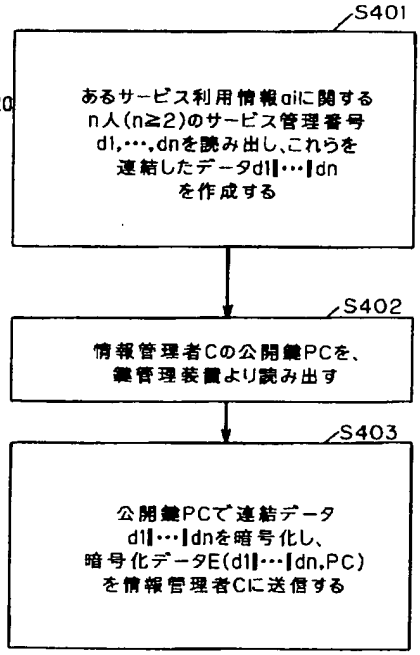
【図２】



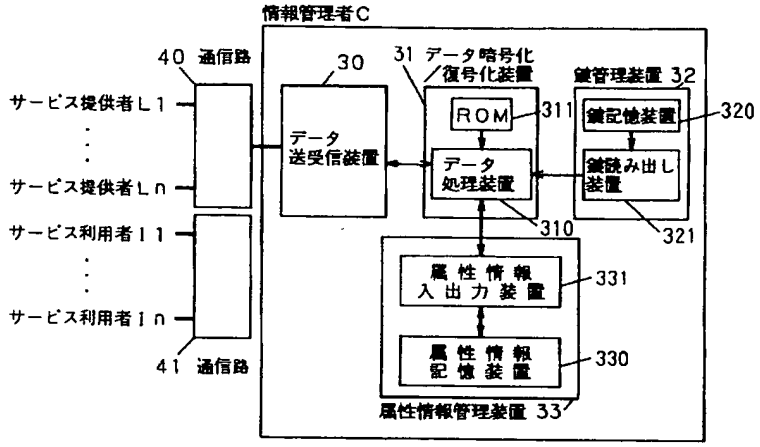
【図３】



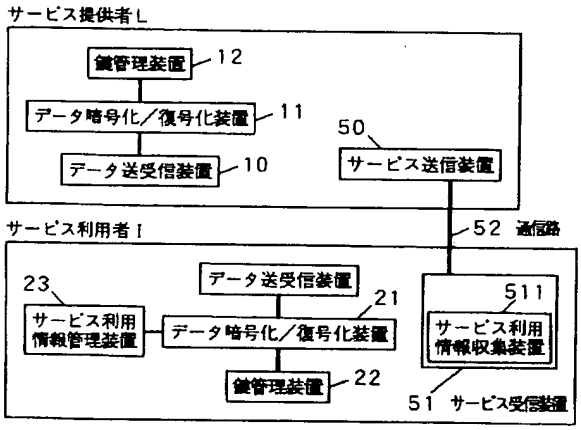
【図１３】



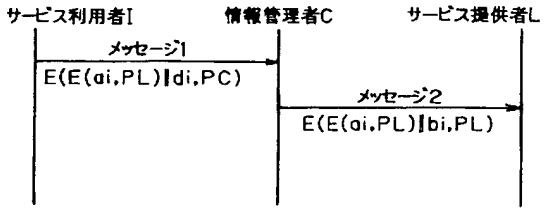
【図４】



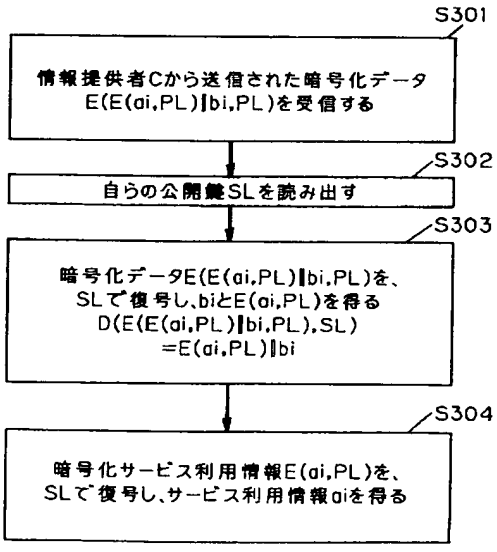
【図５】



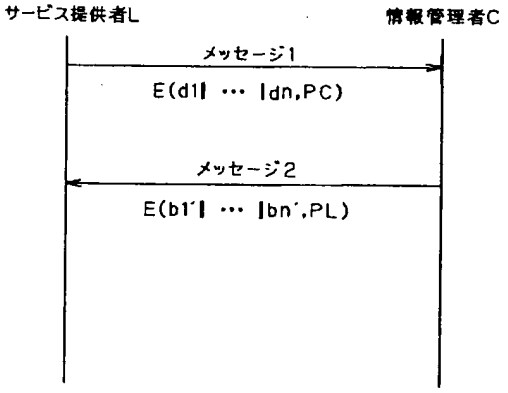
【図６】



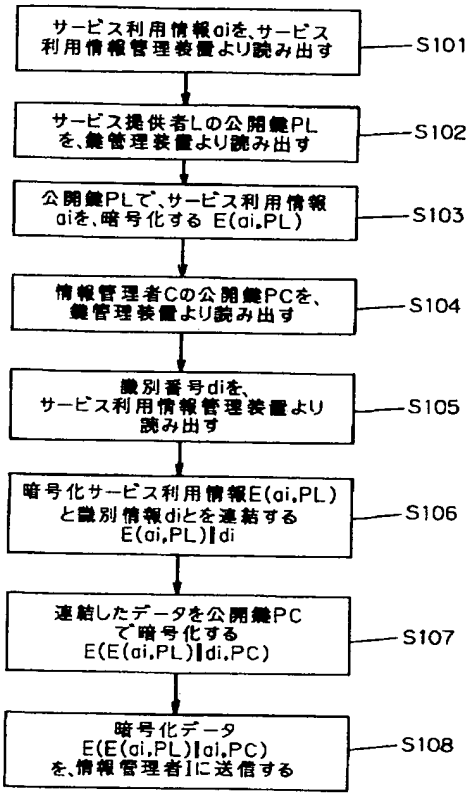
【図９】



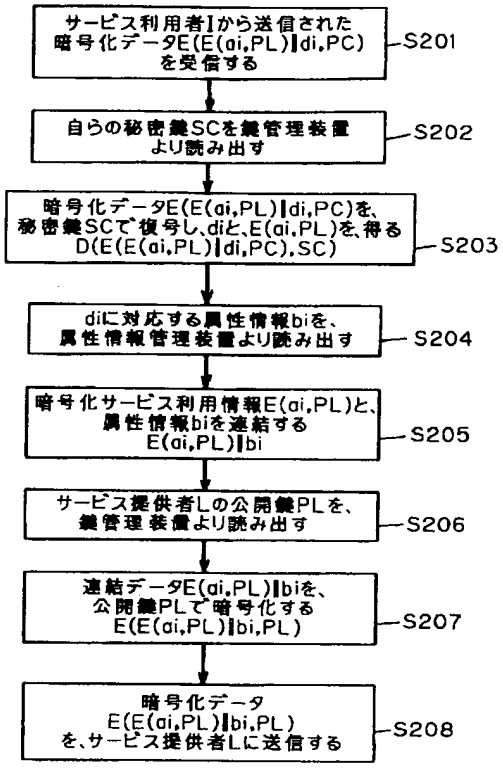
【図１２】



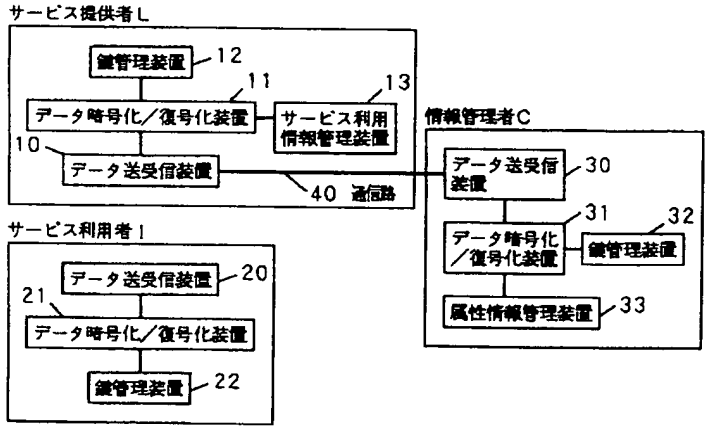
【図７】


サービス利用情報aiを、サービス利用情報管理装置より読み出す
S101
サービス提供者Lの公開鍵PLを、鍵管理装置より読み出す
S102
公開鍵PLで、サービス利用情報aiを、暗号化する E(ai,PL)
S103
情報管理者Cの公開鍵PCを、鍵管理装置より読み出す
S104
識別番号diを、サービス利用情報管理装置より読み出す
S105
暗号化サービス利用情報E(ai,PL)と識別情報diとを連結する E(ai,PL)‖di
S106
連結したデータを公開鍵PCで暗号化する E(E(ai,PL)‖di,PC)
S107
暗号化データ E(E(ai,PL)‖ai,PC)を、情報管理者Iに送信する
S108

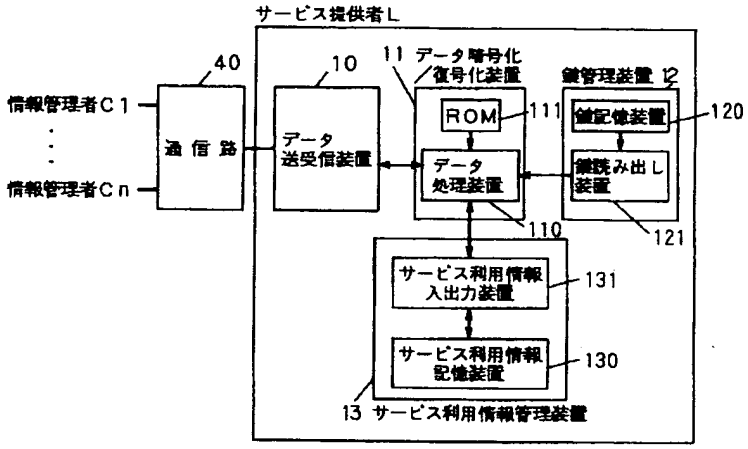
【図８】


サービス利用者Iから送信された暗号化データE(E(ai,PL)‖di,PC)を受信する
S201
自らの秘密鍵SCを鍵管理装置より読み出す
S202
暗号化データE(E(ai,PL)‖di,PC)を、秘密鍵SCで復号し、diと、E(ai,PL)を、得る D(E(E(ai,PL)‖di,PC),SC)
S203
diに対応する属性情報biを、属性情報管理装置より読み出す
S204
暗号化サービス利用情報E(ai,PL)と、属性情報biを連結する E(ai,PL)‖bi
S205
サービス提供者Lの公開鍵PLを、鍵管理装置より読み出す
S206
連結データE(ai,PL)‖biを、公開鍵PLで暗号化する E(E(ai,PL)‖bi,PL)
S207
暗号化データ E(E(ai,PL)‖bi,PL)を、サービス提供者Lに送信する
S208

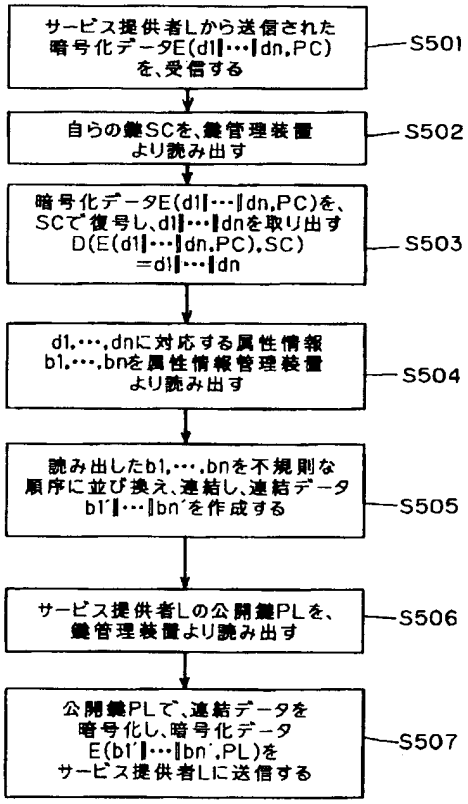
【図１０】


サービス提供者L
鍵管理装置
12
11
13
データ暗号化／復号化装置
サービス利用情報管理装置
10
データ送受信装置
40 通信路
情報管理者C
データ送受信装置
30
31
32
データ暗号化／復号化装置
鍵管理装置
属性情報管理装置
33
サービス利用者I
データ送受信装置
20
21
データ暗号化／復号化装置
鍵管理装置
22

【図１１】


サービス提供者L
40
10
11 データ暗号化/復号化装置
鍵管理装置 12
情報管理者C1
情報管理者Cn
通信路
データ送受信装置
ROM
111
データ処理装置
鍵記憶装置
120
鍵読み出し装置
121
110
サービス利用情報入出力装置
131
サービス利用情報記憶装置
130
13 サービス利用情報管理装置

【図１４】


サービス提供者Lから送信された暗号化データE(d1‖…‖dn,PC)を、受信する
S501
自らの鍵SCを、鍵管理装置より読み出す
S502
暗号化データE(d1‖…‖dn,PC)を、SCで復号し、d1‖…‖dnを取り出すD(E(d1‖…‖dn,PC),SC)=d1‖…‖dn
S503
d1,…,dnに対応する属性情報b1,…,bnを属性情報管理装置より読み出す
S504
読み出したb1,…,bnを不規則な順序に並び換え、連結し、連結データb1'‖…‖bn'を作成する
S505
サービス提供者Lの公開鍵PLを、鍵管理装置より読み出す
S506
公開鍵PLで、連結データを暗号化し、暗号化データE(b1'‖…‖bn',PL)をサービス提供者Lに送信する
S507

フロントページの続き

(51) Int. Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
Ｇ０９Ｃ	1/00	６６０		Ｇ０６Ｆ	15/20	Ｎ
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７５Ｚ